

FIN11: A Widespread Ransomware and Extortion Operation

 brighttalk.com/webcast/7451/447347



Presented by

Genevieve Stark, Threat Analyst, Mandiant Threat Intel; Andrew Moore, Sr. Technical Analyst, Mandiant Threat Intel

About this talk

FIN11 is a financially motivated threat group that delivers malware through widespread and highly successful phishing campaigns that have impacted organizations across sectors and geographies. Mandiant Threat Intelligence has observed FIN11 attempting to monetize their operations at least once using named point-of-sale (POS) malware and, more frequently, using ransomware combined with traditional extortion techniques. In addition to their high-volume spam campaigns, FIN11 is also notable due their consistent evolvement of malware delivery tactics and techniques. Join Genevieve Stark and Andy Moore from Mandiant Threat Intelligence for a look into the motivations, tactics and operations of this newly “graduated” threat group, including the group’s previous activity, common TTPs, and anticipated future focus.

More from this channel

Upcoming talks (**5**)

On-demand talks (**420**)

Subscribers (**91607**)

Mandiant provides public and private organizations and critical infrastructure worldwide with early threat insights through unmatched intelligence and response expertise for the highest-profile incidents.